JUNE 28 - 30, 2005 NORFOLK CONVENTION CENTER

Navy IA Certification Authority

Skip Thaeler

Flag Advisor for Information Assurance

SPAWAR 05

30 June 2005

Sponsored by
SPAWARSYSCOM
FORCEnet Chief Engineer

SPAWAR

Outline

- Terminology
- Certification and Accreditation (C&A) Process
- DITSCAP
- Roles and Responsibilities
- Types of Accreditations
- Types of Certification Efforts
- Certification Approval Workflow
- Workflow Responsibilities
- Documentation
- Resources
- Future Concerns

Terminology

- Certification is the comprehensive evaluation of the technical and non-technical security features of an AIS
- Accreditation is a formal declaration by a Designated Approving Authority (DAA) that an AIS is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk

C&A Process

- Prescribed by the DoDI 5200.40 (DITSCAP)
- Implements policies and procedures for verifying system security architecture
- Builds trust and confidence
- Leads to accreditation

DITSCAP

Phase 1: Definition

- Register System
- Define Roles
- C&A Definition and Analysis

Phase 2: Verification

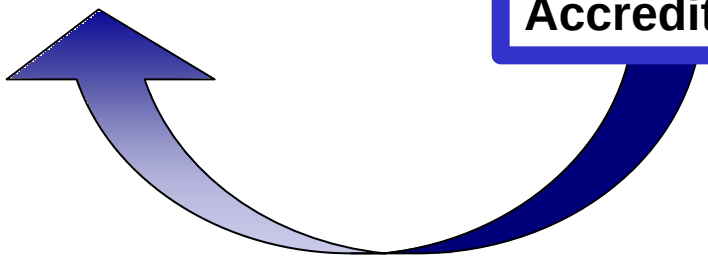
- Verify System Security Architecture (CT&E)
- Verify Design Compliance with Security Requirements
- Evaluate Integrity of Integrated Products

Phase 3: Validation

- Validate System Security Architecture (ST&E)
- Define Residual Risk
- Grant Approval to Operate

Phase 4: Post Accreditation

- Monitor Compliance
- Prepare for Re-accreditation
- Preserve Security Posture



Roles and Responsibilities

- DITSCAP Specifies:
  - Designated Approving Authority (DAA)
    - Formally accepts risk and grants ATO or IATO
  - Certification Authority (CA)
    - Provides accreditation recommendation to DAA
  - Program Management Office (PMO)
    - Funds program and coordinates C&A
  - User Representative
    - Ensures user needs are met

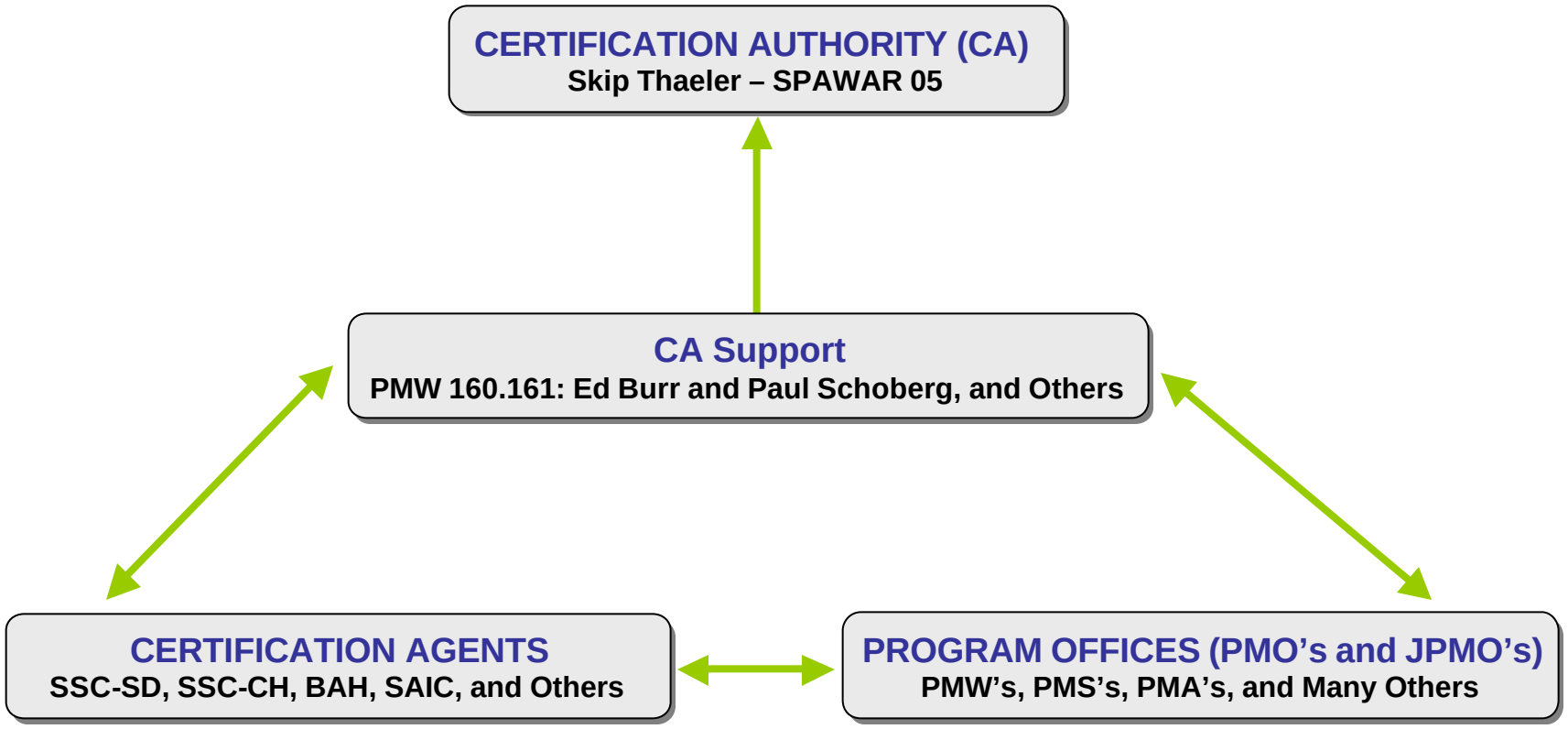
Types of Accreditations

- Classes of Accreditations
  - System Accreditation
  - Type Accreditation
  - Site Accreditation
- Interim Approval to Operate (IATO) for up to 1 year
  - Proof-of-Concept
  - Demonstration
  - Rapid Deployment
  - Where Risk Mitigation is Required
  - Testing
- Approval to Operate (ATO) for up to 3 years

Types of Certification Efforts

- Navy Program of Record (POR)
- Joint Program
- SPAWAR Corporate Enterprise Systems
  - CA support provided based on a handshake agreement between Vanessa Hallihan and Sarah Lamade
- NMCI
  - POR-like efforts
  - Site-like efforts
- Operational/Site (not supported by PMW160)

Certification Approval Workflow



Workflow Responsibilities

- Certification Authority
  - Responsible for making a technical judgment of:
    - System's compliance with security requirements
    - System's security risk
  - Provides guidance to the PMO during the C&A Process
  - Provides accreditation recommendation to DAA

Workflow Responsibilities

- Certification Authority Support
  - Supports Navy CA as PMW 160 C&A
  - Provides guidance to PMs on IA implementation, testing, and documentation efforts
  - Reviews C&A Packages for completeness and accuracy
  - Presents accreditation package to CA for approval

Workflow Responsibilities

- Certification Agents
  - Carry out technical implementation of the DITSCAP
  - ONE CA, but MANY certification agents
    - DON Organizations
    - Other Services
    - Private Companies

Documentation

- System Security Authorization Agreement (SSAA)
  - C&A implementation plan and record
  - Definition of IA architecture and security requirements
  - Evidence of system compliance testing
  - Residual Risk Assessment
- Formal Request for Action
  - Request for Concurrence on SSAA (Phase I)
  - IATO Request (Phase II/III)
  - ATO Request (Phase III)
  - Statement of Accreditation Applicability (Phase II/III/IV)
  - Statement of DITSCAP Non-Applicability (Informal Via Email)

Resources

- Current Personnel Resources (POR, not NMCI)
  - 1 PEO C4I & Space Government
  - 2.25 SSC-SD (includes two full-time x-code support in office)
  - 1 NMCI
  - 2.25 Contractor Support (Document Review & Database)
  - **1 (+) SPAWAR – Certification Authority (+ Alts + TWH Personnel)**
- Shortfalls
  - No Navy CA representation at NAVSEA and NAVAIR
  - No Operational CA resources (Legacy Apps)

Future Concerns

- Staffing
- Funding
- DIACAP
- Expanded Certification Role
- Operational IS Without Accreditation

Questions